UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

FIRST CHOICE FEDERAL CREDIT UNION, AOD FEDERAL CREDIT UNION, TECH CREDIT UNION, VERIDIAN CREDIT UNION, SOUTH FLORIDA EDUCATIONAL FEDERAL CREDIT UNION, PREFERRED CREDIT UNION, ALCOA COMMUNITY FEDERAL CREDIT UNION, ASSOCIATED CREDIT UNION, CENTRUE BANK, ENVISTA CREDIT UNION, FIRST NBC BANK, ALIGN CREDIT UNION, NAVIGATOR CREDIT UNION, THE SEYMOUR BANK, FINANCIAL HORIZONS CREDIT UNION, NORTH JERSEY FEDERAL CREDIT UNION, NUSENDA CREDIT UNION, GREATER CINCINNATI CREDIT UNION, KEMBA FINANCIAL CREDIT UNION, WRIGHT-PATT CREDIT UNION, GREENVILLE HERITAGE FEDERAL CREDIT UNION, and MEMBERS CHOICE CREDIT UNION, on Behalf of Themselves and All Others Similarly Situated, **and** **CREDIT UNION NATIONAL ASSOCIATION, GEORGIA CREDIT UNION AFFILIATES, INDIANA CREDIT UNION LEAGUE, MICHIGAN CREDIT UNION LEAGUE, and OHIO CREDIT UNION LEAGUE,** **Plaintiffs,** **v.** **THE WENDY'S COMPANY, WENDY'S RESTAURANTS, LLC, and WENDY'S INTERNATIONAL, LLC,** **Defendants.**	**Case No. 2:16-cv-00506-NBF-MPK** **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **District Judge Nora Barry Fischer** **Chief Magistrate Judge Maureen P. Kelly**

Plaintiffs First Choice Federal Credit Union, AOD Federal Credit Union, Tech Credit Union, Veridian Credit Union, South Florida Educational Federal Credit Union, Preferred Credit Union, Alcoa Community Federal Credit Union, Associated Credit Union, Centrue Bank, Envista Credit Union, First NBC Bank, Align Credit Union, Navigator Credit Union, The Seymour Bank, Financial Horizons Credit Union, North Jersey Federal Credit Union, Nusenda Credit Union, Greater Cincinnati Credit Union, KEMBA Financial Credit Union, Wright-Patt Credit Union, Greenville Heritage Federal Credit Union, and Members Choice Credit Union ("FI Plaintiffs"), on behalf of themselves and all others similarly situated, and Credit Union National Association, Georgia Credit Union Affiliates, Indiana Credit Union League, Michigan Credit Union League, and Ohio Credit Union League ("Association Plaintiffs"), which are associations that represent the interests of their member credit unions (collectively, the FI Plaintiffs and Association Plaintiffs are referred to as "Plaintiffs"), allege the following against Defendants The Wendy's Company, Wendy's Restaurants, LLC, and Wendy's International, LLC (collectively, "Wendy's," the "Company," or "Defendants"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

I. INTRODUCTION

1. Plaintiffs bring this class action on behalf of financial institutions that suffered, and continue to suffer, financial losses as a direct result of Wendy's conscious failure to take adequate and reasonable measures to protect its point-of-sale and computer systems. Wendy's actions left highly sensitive Payment Card Data, including, but not limited to, the cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code ("Payment Card Data"), of hundreds of thousands, if not millions, of the FI Plaintiffs' customers exposed and accessible for use by hackers for months. As a result, the FI Plaintiffs have incurred significant

damages in replacing customers' payment cards and covering fraudulent purchases, among other things.

2. In or about October 2015, computer hackers accessed Wendy's inadequately protected point-of-sale systems and installed malicious software (often referred to as "malware") that infected over 1,000 Wendy's restaurants in the United States. Through this malware, hackers stole the Payment Card Data of an untold number of customers. The stolen Payment Card Data then was sold on the internet to individuals who made massive numbers of fraudulent transactions on payment cards that the FI Plaintiffs and other members of the Class (as defined below) issued to Wendy's customers.

3. The data breach was the inevitable result of Wendy's inadequate data security measures and lackadaisical approach to the security of its customers' Payment Card Data. Despite the well-publicized and ever-growing threat of cyber-attacks targeting Payment Card Data through vulnerable point-of-sale systems and inadequately protected computer networks, Wendy's refused to implement certain best practices, failed to upgrade critical security systems, used outdated point-of-sale systems, ignored warnings about the vulnerability of its computer network, and disregarded and/or violated applicable industry standards.

4. Wendy's data security deficiencies were further buttressed by Wendy's failure to timely identify the breach and subsequently contain it. By February 2016, when Wendy's first publicly acknowledged that a data breach compromising customer Payment Card Data had occurred, the data breach already had been ongoing for several months. The malware had remained undetected within Wendy's point-of-sale and computer systems from October 2015 until late January 2016, when third parties first notified Wendy's that an unusual number of potentially fraudulent transactions had taken place on payment cards recently used at Wendy's restaurants.

5. Although Wendy's claimed that it immediately began an investigation when it learned of the data breach, its security deficiencies were so significant that Wendy's not only failed to timely notify financial institutions that their payment cards were at risk, but also failed to take proper measures to contain the data breach and prevent ongoing and subsequent exfiltration of Payment Card Data.

6. Wendy's initially announced that the malware discovered on its point-of-sale systems was limited and impacted only 300 of the Company's more than 5,500 U.S. restaurants. Wendy's further suggested that, as of May, 2016, the source of the malware had been identified, disabled, and eradicated.

7. Wendy's now admits, however, that the impact of the data breach was much more widespread than previously disclosed, that malware was identified at over 1,000 restaurants (more than triple the original representation), and that the data breach was nationwide in scope, impacting all but four states and the District of Columbia.[1]

8. Furthermore, the fraud exposure window, when Payment Card Data was at risk, is much longer than what Wendy's initially disclosed. For example, Visa initially stated that the fraud exposure window ran from October 26, 2015 through February 14, 2016, but later extended the ending date of the exposure window by more than four months – to June 25, 2016 – meaning the breach was not contained for nearly ***six months*** after Wendy's was notified the malware was on its systems.

---

[1] *See* WENDY'S.COM, https://payment.wendys.com/paymentcardcheck.html (last visited July 21, 2016) (a review of Wendy's notice website regarding the breach indicates that restaurants in every state have been impacted except Delaware, Maryland, Mississippi, Vermont, and Washington D.C.). Considering that the data breach continues to expand, it is entirely possible that locations in these remaining states also have been or will be impacted.

9. Despite Wendy's claim that the data breach has been contained, Plaintiffs believe that the breach remains ongoing to date. Indeed, the FI Plaintiffs and other members of the Class continue to suffer new, recent losses as a result of the data breach.

10. The financial costs caused by Wendy's deficient data security approach have been borne primarily by financial institutions, like the FI Plaintiffs, that issued the payment cards compromised in the data breach. These costs include, but are not limited to, canceling and reissuing compromised cards and reimbursing their customers for fraudulent charges. Industry sources estimate that the fraudulent charges from this breach have been even more pervasive than in other recent data breaches (*e.g.*, Target and Home Depot), causing the FI Plaintiffs and other members of the Class to suffer much greater losses than were suffered by financial institutions in connection with those breaches.[2] Moreover, the duration of the data breach and Wendy's inadequate response thereto have caused the FI Plaintiffs and other members of the Class to suffer many millions of dollars more in damages than they would have suffered had Wendy's had an adequate process in place to detect the breach and/or actually contain the data breach when Wendy's first learned of it.

11. This class action is brought on behalf of financial institutions throughout the U.S. to recover the damages that they and others similarly situated have suffered, and continue to suffer, as a direct result of the Wendy's data breach. The FI Plaintiffs assert claims for negligence, negligence *per se*, violation of the Ohio Deceptive Trade Practices Act, Ohio Code §§ 4165.01, *et seq*., and declaratory and injunctive relief.

[2] For instance, in Home Depot, 56 million payment cards were exposed as a result of the Home Depot data breach.

12. The Association Plaintiffs, whose members were damaged by the Wendy's data breach, also join this action. The Association Plaintiffs do not seek damages, but only equitable declaratory and injunctive relief on behalf of their respective members and not as class representatives.

II. PARTIES

A. FI Plaintiffs

13. Plaintiff First Choice Federal Credit Union is a federally chartered credit union with its principal place of business located in New Castle, Pennsylvania. As a result of the Wendy's data breach, Plaintiff First Choice Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

14. Plaintiff AOD Federal Credit Union is a federally chartered credit union with its principal place of business located in Oxford, Alabama. As a result of the Wendy's data breach, Plaintiff AOD Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

15. Plaintiff Tech Credit Union is an Indiana-chartered credit union with its principal place of business located in Crown Point, Indiana. As a result of the Wendy's data breach, Plaintiff Tech Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to

investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

16. Plaintiff Veridian Credit Union is an Iowa-chartered credit union with its principal place of business located in Waterloo, Iowa. As a result of the Wendy's data breach, Plaintiff Veridian Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

17. Plaintiff South Florida Educational Federal Credit Union is a federally chartered credit union with it principal place of business located in Miami, Florida. As a result of the Wendy's data breach, Plaintiff South Florida Educational Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

18. Plaintiff Preferred Credit Union is a Michigan-chartered credit union with its principal place of business located in Grand Rapids, Michigan. As a result of the Wendy's data breach, Plaintiff Preferred Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

19. Plaintiff Alcoa Community Federal Credit Union is a federally chartered credit union with its principal place of business located in Benton, Arkansas. As a result of the Wendy's

data breach, Plaintiff Alcoa Community Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

20. Plaintiff Associated Credit Union is a Georgia-chartered credit union with its principal place of business located in Norcross, Georgia. As a result of the Wendy's data breach, Plaintiff Associated Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

21. Plaintiff Centrue Bank is an Illinois-chartered bank with its principal place of business located in Ottawa, Illinois. As a result of the Wendy's data breach, Plaintiff Centrue Bank has suffered and continues to suffer injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

22. Plaintiff Envista Credit Union is a Kansas-chartered credit union with its principal place of business located in Topeka, Kansas. As a result of the Wendy's data breach, Plaintiff Envista Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

23. Plaintiff First NBC Bank is a Louisiana-chartered bank with its principle place of business located in New Orleans, Louisiana. As a result of the Wendy's data breach, Plaintiff First

NBC Bank has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

24. Plaintiff Align Credit Union is a Massachusetts-chartered credit union with its principal place of business located in Lowell, Massachusetts. As a result of the Wendy's data breach, Plaintiff Align Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

25. Plaintiff Navigator Credit Union is a Mississippi-chartered credit union with its principal place of business located in Pascagoula, Mississippi. As a result of the Wendy's data breach, Plaintiff Navigator Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

26. Plaintiff The Seymour Bank is a Missouri-chartered bank with its principle place of business located in Seymour, Missouri. As a result of the Wendy's data breach, Plaintiff The Seymour Bank has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

27. Plaintiff Financial Horizons Credit Union is a Nevada-chartered credit union with its principal place of business located in Hawthorne, Nevada. As a result of the Wendy's data breach, Plaintiff Financial Horizons Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

28. Plaintiff North Jersey Federal Credit Union is a federally chartered credit union with its principle place of business located in Totowa, New Jersey. As a result of the Wendy's data breach, Plaintiff North Jersey Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

29. Plaintiff Nusenda Credit Union is a federally chartered credit union with its principle place of business in Albuquerque, New Mexico. As a result of the Wendy's data breach, Plaintiff Nusenda Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

30. Plaintiff Greater Cincinnati Credit Union is an Ohio-chartered credit union with its principle place of business located in Cincinnati, Ohio. As a result of the Wendy's data breach, Plaintiff Greater Cincinnati Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund

fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

31. Plaintiff KEMBA Financial Credit Union is an Ohio-chartered credit union with its principle place of business located in Gahanna, Ohio. As a result of the Wendy's data breach, Plaintiff KEMBA Financial Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

32. Plaintiff Wright-Patt Credit Union is an Ohio-chartered credit union with its principal place of business located in Beavercreek, Ohio. As a result of the Wendy's data breach, Plaintiff Wright-Patt Credit Union has suffered and continues to suffer injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

33. Plaintiff Greenville Heritage Federal Credit Union is a federally chartered credit union with its principle place of business located in Greenville, South Carolina. As a result of the Wendy's data breach, Plaintiff Greenville Heritage Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

34. Plaintiff Members Choice Credit Union is a Texas-chartered credit union with its principal place of business located in Houston, Texas. As a result of the Wendy's data breach, Plaintiff Members Choice Credit Union has suffered, and continues to suffer, injury, including,

inter alia, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

35. Each FI Plaintiff is at risk of imminent and certain impending injury by the apparent ongoing nature of the data breach, as several FI Plaintiffs report that they continue to experience losses, as a result of recurrent fraudulent transactions on payment cards linked to the Wendy's data breach. Furthermore, each FI Plaintiff is subject to an imminent threat of future harm because Wendy's response to the data breach has been so inadequate that it is doubtful that it has cured the deficiencies in its data security measures sufficiently to prevent a subsequent data breach.

B. Association Plaintiffs

36. The Association Plaintiffs are associations whose members were, and continue to be, damaged as a result of the Wendy's data breach and likely will suffer further damage if another breach occurs. Given Wendy's inability to timely contain the data breach, it is doubtful that the breach now has been contained. Furthermore, it is uncertain whether Wendy's has cured the ongoing data security deficiencies. If those deficiencies have not been cured, the Association Plaintiffs are substantially likely to suffer injury in the future. The Association Plaintiffs are non-class plaintiffs. While the Association Plaintiffs have themselves been injured by the Wendy's data breach, they do not seek money damages. Rather, the Association Plaintiffs bring this action for equitable relief on behalf of their members and have standing to do so because their members would otherwise have standing to sue in their own right; the interests they seek to protect are germane to their respective purposes; and the relief sought does not require participation of individual members. The Association Plaintiffs are as follows:

37. Plaintiff Credit Union National Association ("CUNA"), dual-headquartered in Washington, D.C. and Wisconsin, is the largest association of credit unions in the U.S. Credit unions are not-for-profit cooperatives providing financial services to people from all walks of life and are owned by the consumers that the credit unions serve. CUNA represents approximately 5,000 credit unions. The nation's credit unions are owned by more than 100 million memberships throughout the U.S. CUNA's purpose includes representing and serving the interests of its members by, *inter alia*, organizing and focusing their advocacy efforts; providing education and training; and serving as a forum for its members to meet and share ideas regarding their operations and industry.

38. Plaintiff Georgia Credit Union Affiliates ("Georgia CUA") is an association of credit unions headquartered in Georgia. Georgia CUA represents 133 credit unions with combined assets of more than $19 billion. Georgia CUA's purpose includes advocating for its members and assisting its members to become the premier source of financial services for Georgians.

39. Plaintiff Indiana Credit Union League ("Indiana CUL") is an association of credit unions headquartered in Indiana. Indiana CUL has over 170 member credit unions, which have approximately $21.5 billion in assets and are owned by more than two million consumers throughout Indiana. Indiana CUL's purpose is to help credit unions through advocacy to protect and further its members' interests by offering consultation, legislative, and regulatory support and by providing public relations, operational and technical assistance, education, and training.

40. Plaintiff Michigan Credit Union League ("Michigan CUL") is an association of credit unions headquartered in Michigan. Michigan CUL has over 240 member credit unions, which have approximately $52 billion in assets and are owned by nearly five million consumers throughout Michigan. Michigan CUL's purpose is to help credit unions through advocacy to

protect and further its members' interests by offering consultation, legislative, and regulatory support and by providing public relations, operational and technical assistance, education, and training.

41. Plaintiff Ohio Credit Union League ("Ohio CUL") is an association of credit unions headquartered in Ohio. Ohio CUL's credit union members have over $8 billion in assets and are owned by approximately 2.76 million consumers. Ohio CUL's purpose includes advocating for its members and providing them with compliance and information services, opportunities for educational and professional development, communications, media relations, and outreach.

42. The Association Plaintiffs are duly authorized to bring this action against Wendy's. Many of the Association Plaintiffs' members do not have the time or resources to pursue this litigation and, in many instances, fear retribution if they become named plaintiffs. Wendy's has caused the Association Plaintiffs to expend their own resources to educate and assist injured members in handling and appropriately responding to the Wendy's data breach and they have otherwise been directly and adversely impacted.

C. Defendants

43. Defendant The Wendy's Company is a Delaware corporation with its principal place of business in Dublin, Ohio.

44. Defendant Wendy's Restaurants, LLC is a Delaware limited liability company with its principal place of business in Dublin, Ohio, whose sole member is The Wendy's Company.

45. Defendant Wendy's International, LLC is an Ohio limited liability company with its principal place of business in Dublin, Ohio, whose parent company is Wendy's Restaurants, LLC.

46. Wendy's is engaged in the business of operating, developing, and franchising a system of quick-service restaurants. According Wendy's Form 10-K filed with the Securities and Exchange Commission ("SEC") for the fiscal year ended January 3, 2016 ("2015 Form 10K"), "Wendy's restaurant system was comprised of 6,479 restaurants, of which 632 were owned and operated by the Company."[3] In 2015, its revenues totaled approximately $1.9 billion. *Id*.

47. As a franchisor, Wendy's has total control over the manner in which its franchisees operate in order to maintain uniformity from restaurant to restaurant across the country. Wendy's standard form Unit Franchise Agreement emphasizes the importance of "uniform standards, specifications, and procedures for operations[,]" any aspect of "which may be changed, improved, and further developed by [Wendy's] from time to time[.]"[4] The Unit Franchise Agreement indicates that Wendy's control over franchisee operations extends to "computer software and electronic data transmission systems for point of sale reporting." *Id*.

48. Similarly, the Company's 2015 Form 10-K also stated that:

> Franchised restaurants are required to be operated under uniform operating standards and specifications relating to the selection, quality and preparation of menu items, signage, decor, equipment, uniforms, suppliers, maintenance and cleanliness of premises and customer service. Wendy's monitors franchisee operations and inspects restaurants periodically to ensure that required practices and procedures are being followed.[5]

---

[3] The Wendy's Co., Annual Report (Form 10-K) (Mar. 3, 2016), https://www.sec.gov/Archives/edgar/data/30697/000030697160000011/twc10k2015.htm.

[4] The Wendy's Co., Annual Report (EX-10.22 to Form 10-K) (Mar. 3, 2016), https://www.sec.gov/Archives/edgar/data/1548621/000154862113000033/exhibit1022wendysformagree.htm.

[5] The Wendy's Co., Annual Report (Form 10-K) (Mar. 3, 2016), https://www.sec.gov/Archives/edgar/data/30697/000030697160000011/twc10k2015.htm.

49. According to a lawsuit filed by Wendy's against one of its franchisees, *Wendy's Int'l, LLC v. DavCo Rests. LLC*, No. 14CV013382 (Ohio Ct. Comm. Pl.) (the "*DavCo* lawsuit") (attached as Exhibit 1), Wendy's admits that the "guidelines announced by Wendy's [are] to be followed by all U.S. and Canadian franchisees" and are "key obligations at the core of the franchisor/franchisee relationship between Wendy's and [the franchisee]." Ex. 1, ¶1. Specifically, Wendy's avers that "these obligations [include the requirement] for all U.S. and Canadian franchisees (a) to purchase and install a common point of sale computer platform." *Id.*

50. With regard to its total control over franchisee operations, Wendy's alleges in the *DavCo* lawsuit:

> The essence of any franchisor/franchisee relationship is that in exchange for the grant of a franchise, . . . the franchisee agrees, among other things, to follow the processes and maintain the standards established by the franchisor. . . . The Franchise Agreements between Wendy's and [its franchisees] make clear that Wendy's "has developed and owns a distinctive format and system relating to the establishment and operation of Wendy's Old fashioned Hamburgers restaurants" (Franchise Agreements, first WHEREAS clause), and that [the franchisee] "understands and acknowledges the importance of [Wendy''s] high standards of quality, cleanliness, appearance, and service, and ***the necessity of operating the business franchised hereunder in conformity with [Wendy's] standards and specifications***." (Franchise Agreements, sixth WHEREAS clause.)

Ex. 1, ¶¶9-10. *See also id.*, Ex. A at 6, 8-9, Franchise Agreement, §§6.1, 6.11, 6.13. The Franchise Agreement specifically obligates franchisees to purchase, install, and utilize fixtures, furnishings, and equipment that may be specified by Wendy's from time to time. *Id.*, ¶12 (quoting Ex. A at 8-9, Franchise Agreement, §§6.11.C, 6.17).

III. JURISDICTION AND VENUE

51. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d), because at least one Class member is of diverse

citizenship from one defendant, there are more than 100 Class members, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs.

52. The Western District of Pennsylvania has personal jurisdiction over Defendants named in this action because Defendants conduct substantial business in this District.

53. Venue is proper in this District under 28 U.S.C. §1391(b) because at least one of the Defendants resides in this District, a substantial part of the events or omissions giving rise to the claims occurred in this District, and Defendants have caused harm to Class members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Payment Card Processing Background

54. It is well known that customer Payment Card Data is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including The Home Depot, Target, Kmart, P.F. Chang's, and many others. Despite widespread publicity and industry alerts regarding these other notable data breaches, Wendy's failed to take reasonable steps to adequately protect its computer systems from being breached.

55. A large portion of Wendy's sales are made to customers who use credit or debit cards. When a customer uses a credit or debit card, the transaction involves four primary parties: (1) the "merchant" (*e.g.*, Wendy's) where the purchase is made; (2) an "acquiring bank" (which typically is a financial institution that contracts with the merchant to process its payment card transactions); (3) a "card network" or "payment processor" (such as Visa and MasterCard); and (4) the "issuer" (which is a financial institution – such as Plaintiffs – that issues credit and debit cards to its customers).

56. Processing a payment card transaction involves four major steps:

- *Authorization* – when a customer presents a card to make a purchase, Wendy's requests authorization of the transaction from the card's issuer;
- *Clearance* – if the issuer authorizes the transaction, Wendy's completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted;
- *Settlement* – the acquiring bank pays Wendy's for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank; and
- *Post-Settlement* – the issuer posts the charge to the customer's credit or debit account.

57. In processing payment card transactions, merchants acquire a substantial amount of information about each customer, including his or her full name; credit or debit card account number; card security code (the value printed on the card or contained in the microprocessor chip or magnetic strip of a card and used to validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards. This information typically is stored on the merchants' computer systems and transmitted to third parties to complete the transaction. At other times, and for other reasons, merchants may also collect other personally identifiable information about their customers, including, but not limited to, financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses.

58. For years, Wendy's has stored in its computer systems massive amounts of customer Payment Card Data. Wendy's uses this information to process payment card transactions in connection with sales to its customers and to generate profits by sharing the information with third-party affiliates, recommending additional services to customers, and employing predictive

marketing techniques. In sum, customer Payment Card Data is an asset of considerable value to both the Company and to hackers, who can easily sell this data, as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[6]

59. Wendy's is – and at all relevant times has been – aware that the Payment Card Data it maintains is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

60. Wendy's also is – and at all relevant times has been – aware of the importance of safeguarding its customers' Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, specifically including the significant costs that would be imposed on issuers, such as the FI Plaintiffs, and others.

61. In addition to its general duty to safeguard customers' Payment Card Data to prevent the risk of foreseeable harm to others, Wendy's is – and at all relevant times has been – obligated to safeguard such information by, among other things, industry standards, federal law, and its own commitments, internal policies, and procedures.

B. The Wendy's Data Breach: October 2015 to Present

62. Beginning in approximately October 2015, computer hackers took advantage of the numerous vulnerabilities in Wendy's computer and point-of-sale systems by using the credentials of a third-party vendor to install malware that ultimately infected at least 1,000 restaurants across the U.S. Through this malware, the hackers were able to steal Wendy's customers' Payment Card Data that Wendy's had collected in conjunction with its customers' restaurant purchases.

---

[6] *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016, 10:47 AM), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited July 22, 2016).

63. By December 2015, Wendy's knew that a data breach was impacting many of its locations. A former Wendy's employee, who worked as a Field Network/System Administrator ("System Admin"), and another former high ranking employee in Wendy's Technology Solutions group ("Tech Solutions Employee 1") both independently stated that they were informed in December 2015 that a data breach was ongoing at that time. Despite its knowledge of the data breach in December 2015, Wendy's failed to disclose to Plaintiffs or the general public that a data breach had occurred.

64. By early January 2016, unauthorized charges on payment cards used at Wendy's locations already were well under way. One customer noted that she suspected that her credit card information was stolen in early January after visiting a Wendy's in Illinois. And, in late January, news sources reported that a data breach had likely occurred after some banks noticed a pattern of fraud on payment cards that all recently had been used at Wendy's restaurants.[7]

65. On January 27, 2016 (at least a month after it already knew of the breach), Wendy's finally announced that it was investigating reports of '"unusual activity'" on payment cards used in some of its restaurants, but refused to acknowledge that a data breach had occurred, reiterating that "it is difficult to determine with certainty the nature or scope of any potential incident."[8]

66. It was not until February 9, 2016, nearly two weeks after the public reports surfaced, that Wendy's finally publicly acknowledged that "some [of its locations] have been found by the

---

[7] *Wendy's Probes Reports of Credit Card Breach*, KREBS ON SECURITY (Jan. 27, 2016, 9:17 AM), http://krebsonsecurity.com/2016/01/wendys-probes-reports-of-credit-card-breach/ (last visited July 22, 2016).

[8] *Wendy's Investigating Reports of 'Unusual Activity' on Payment Cards Used at Some Restaurants*, WALL ST. J. (Jan. 27, 2016, 11:23 AM), http://www.wsj.com/articles/wendys-investigating-reports-of-unusual-activity-on-payment-cards-used-at-some-restaurants-1453911780 (last visited July 22, 2016).

cybersecurity experts to have malware on their systems."[9] Attempting to downplay the seriousness of the data breach, Wendy's assured its customers that financial institutions – like the FI Plaintiffs and other members of the Class – would reimburse Wendy's customers for any fraudulent charges.

67. On February 26, 2016, Visa issued a Compromised Account Management System ("CAMS") alert to at least some financial institutions, indicating that the estimated fraud "exposure window" for the Wendy's data breach ran from October 26, 2015 through February 14, 2016. The CAMS alert further indicated that both Track 1 and Track 2 data, which generally includes credit and debit card information, such as cardholder name, primary account number, and in certain instances, PIN number, may have been compromised in the data breach. MasterCard issued a similar alert on March 7, 2016.

68. In its 2015 Form 10-K, Wendy's stated:

> the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity at some Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on a certain system. The investigation is ongoing and the Company is continuing to work closely with cybersecurity experts and law enforcement officials.[10]

69. On April 1, 2016, Visa issued another CAMS alert to at least some financial institutions, indicating that the estimated fraud exposure window for the Wendy's data breach ran from October 26, 2015 through March 10, 2016 – extending the fraud exposure window by nearly a month more than previously disclosed.

---

[9] The Wendy's Co., Current Report (EX-99.1 to Form 8-K) (Feb. 9, 2016), https://www.sec.gov/Archives/edgar/data/30697/000119312516454484/d120464dex991.htm (last visited July 22, 2016).

[10] The Wendy's Co., Annual Report (EX-99.1 to Form 10-K) (Mar. 3, 2016), https://www.sec.gov/Archives/edgar/data/30697/000003069716000011/twc10k2015.htm (last visited July 22, 2016).

70. On May 10, 2016, Visa again issued a CAMS alert to at least some financial institutions, extending both the beginning and end date of the fraud exposure window for the Wendy's data breach to August 31, 2015 through April 1, 2016.

71. On May 11, 2016, Wendy's issued a press release on Form 8-K filed with the SEC. In this press release, Wendy's acknowledged that "several hundred" of its restaurants were impacted by "malware" that was "installed through the use of compromised third-party vendor credentials" that "affected one particular point of sale system."[11] The press release went on to state that Wendy's along with its cybersecurity experts had "disabled and eradicated the malware in affected restaurants." *Id*. This was false.

72. On June 9, 2016, Wendy's issued another press release on Form 8-K filed with the SEC. In this press release, Wendy's disclosed that the data breach was much larger than Defendants had first reported. Specifically, Wendy's explained that "***the Company has recently discovered a variant of the malware[.] . . . This malware has been discovered on some franchise restaurants' [point-of-sale] systems, and the number of franchise restaurants impacted by these cybersecurity attacks is now expected to be considerably higher***" than Defendants' previous estimates.[12] [Emphasis added].

73. Defendants' June 9, 2016 press release further intimated that the data breach remained ongoing, still causing substantial damages to the FI Plaintiffs and other members of the Class. This would mean that Wendy's failed to identify and contain the data breach to stop the

---

[11] The Wendy's Co., Current Report (EX-99.1 to Form 8-K) (May 11, 2016), https://www.sec.gov/Archives/edgar/data/30697/000119312516586362/d158377dex991.htm (last visited July 22, 2016).

[12] The Wendy's Co., Current Report (EX-99.1 to Form 8-K) (June 9, 2016), https://www.sec.gov/Archives/edgar/data/30697/000119312516617956/d121680dex991.htm (last visited July 22, 2016).

hackers from stealing Payment Card Data ***for approximately eight months***. Indeed, despite Wendy's claims that the malware had been identified and the breach contained, Plaintiffs believe that the breach remains ongoing through the date of this filing, as the FI Plaintiffs continue to suffer fraud losses and have had to continue to canceling and reissuing their customers' payment cards in connection with the Wendy's data breach.

74. On July 7, 2016, Wendy's issued yet another press release identifying the specific Payment Card Data that had been targeted by hackers:

> Working closely with third-party forensic experts, federal law enforcement and payment card industry contacts as part of its ongoing investigation, the Company has determined that specific payment card information was targeted by the additional malware variant. ***This information included cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code***.[13]

[Emphasis added].

Todd Penegor, Wendy's President and Chief Executive Officer ("CEO"), stated:

> We are committed to protecting our customers and keeping them informed. We sincerely apologize to anyone who has been inconvenienced as a result of these highly sophisticated, criminal cyberattacks involving some Wendy's restaurants. . . . We have conducted a rigorous investigation to understand what has occurred and apply those learnings to further strengthen our data security measures.[14]

75. Wendy's again confirmed the breach occurred through a compromise of the security credentials from one of its service providers, which thereby allowed the hackers to deploy the malware and access Payment Card Data from point-of-sale systems. This was the exact same highly publicized process by which Target had been breached only a few years before. Wendy's

---

[13] Press Release, The Wendy's Company, Wendy's Update on Payment Card Security Incident (July 7, 2016), http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2182670 (last visited July 22, 2016).

[14] *Id.*

further confirmed that malware at issue was placed on Wendy's franchisee systems starting in late Fall of 2015. *Id*.

76. On July 8, 2016, Visa issued a subsequent CAMS alert extending the ending date for the fraud exposure window into late June 2016. On July 8, 2016, MasterCard also issued a revised Account Data Compromise ("ADC") alert indicating that the exposure window was between December 1, 2015 and June 10, 2016 and included both Track 1 and Track 2 data.

77. On July 8, 2016, the *Pittsburgh Post-Gazette* reported that several Wendy's restaurants in the Pittsburgh region were among the more than 1,000 Wendy's locations in the U.S. where personal and financial data was compromised. Specifically, the report states that "Wendy's said hackers were able to steal customers' credit and debit card information at 1,025 of its U.S. restaurants, far more than it originally thought. The hamburger chain said hackers were able to obtain card numbers, names, expiration dates and codes on the card, beginning in late fall."[15]

78. Taking advantage of Wendy's lax data security and delayed notification to financial institutions and the public, hackers were able to gather large amounts of Payment Card Data. With that Payment Card Data, unknown perpetrators were able to make a significant number of undetected fraudulent purchases on credit and debit cards that had been issued by the FI Plaintiffs and members of the Class. Unknown perpetrators also specifically targeted and drained debit accounts with large amounts of money in them, concentrating the damages and causing individual financial institutions, such as the FI Plaintiffs and members of the Class, significant losses. By failing to timely identify, and then publicly acknowledge, that its systems had been subjected to a

[15] Patricia Sabatini, *Wendy's IDs Pittsburgh-area restaurants hit by payment card breach*, PITTSBURGH POST-GAZETTE (July 8, 2016, 11:18 AM), http://www.post-gazette.com/business/pittsburgh-company-news/2016/07/08/Wendy-s-IDs-13-Pittsburgh-area-restaurants-hit-by-payment-card-breach/stories/201607080162.print (last visited July 22, 2016).

data breach, and then failing to timely contain the data breach, Wendy's allowed hackers to have unfettered access to Wendy's computer and point-of-sale systems to obtain customers' Payment Card Data for at least eight months, thereby exponentially increasing the harm suffered by the FI Plaintiffs and members of the Class.

79. Up to, and including, the period during which the Wendy's data breach occurred, Wendy's data security systems suffered from many deficiencies that made them susceptible to hackers, including, without limitation, the following:

a. Wendy's IT management were unqualified and failed to maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. Wendy's ignored well-known warnings that its point-of-sale system was susceptible to data breach;

c. Wendy's customization of its point-of-sale systems frequently compromised Wendy's point-of-sale and security systems, requiring Wendy's, at times, to disable software that provided malware detection and other security functions, which left Payment Card Data unprotected;

d. Wendy's operated its point-of-sale systems on an outdated operating system, which was highly vulnerable to attack because the manufacturer no longer provided security or technical updates;

e. Wendy's lacked adequate firewall protection and proper network segmentation, which would have prevented hackers from accessing Payment Card Data;

f. Wendy's failed to implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its point-of-sale and other systems that accessed Payment Card Data and otherwise would have protected Payment Card Data;

g. Wendy's failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented Payment Card Data from being stolen; and

h. Wendy's failed to upgrade its payment systems to utilize EMV technology, which would have provided better security for Payment Card Data.

C. Numerous Deficiencies in Wendy's IT and Security Systems Caused Wendy's to Be Susceptible to a Data Breach

1. Despite Well-Known Risks, Wendy's Lackadaisical Approach to Data Security Contributed to the Data Breach

80. Much of the blame for the state of Wendy's data security systems can be placed squarely on the shoulders of the Company's IT management, who were incompetent and failed to maintain a system of accountability over data security. Indeed, Wendy's senior management were aware of the primary security deficiencies that left Payment Card Data at risk, yet failed to take the necessary steps to remediate such deficiencies.

81. Wendy's corporate culture towards data security was best described by a former Senior Engineer ("Senior Engineer 2"), who stated that the IT managers at Wendy's took a "hope for the best" attitude towards security. Senior Engineer 2 further stated that Wendy's IT personnel, including those in upper management, "had no clue what they were doing" and frequently addressed issues in ways that weakened system security, rather than strengthened it.

82. Senior Engineer 2 worked out of Wendy's corporate headquarters between 2014 and 2015 and initially reported to the Chief Engineer of IT Infrastructure, Jim Gatto, and subsequently to the Director of Store Technology, Phil Newson. Senior Engineer 2 stated that the there was a general lack of accountability in the IT department at Wendy's and the IT personnel lacked both proper training and a solid understanding of how Wendy's IT systems operated.

83. Senior Engineer 2 emphasized that the IT department routinely failed to address known security issues. For example, he explained that IT management continued to use the Windows XP operating system for the Aloha point-of-sale ("Aloha POS") system (Wendy's internal point-of-sale system, discussed more fully below) despite well-known vulnerabilities. Windows XP was an outdated operating system that Microsoft no longer supported with security and technical updates. Senior Engineer 2 stated that when he raised concerns with IT employees regarding the continued use of Windows XP, these employees would act surprised and horrified that Windows XP was in use, yet never would do anything to rectify the problem.

84. Senior Engineer 2 also stated that managers of the IT and security systems were often more concerned about sticking to their project timelines than they were about ensuring the security of their systems, regularly sacrificing the latter in favor of meeting their deadlines.

85. Wendy's was clearly aware of the threat of a data breach given the prior high-profile breaches that occurred at Target, Home Depot, and others. Indeed, Visa warned merchants, including Wendy's, as early as August 2013 of malware targeting point-of-sale systems. Specifically, the alert, entitled "Retail Merchants Targeted by Memory-Parsing Malware," warned: "Since January 2013, Visa has seen an increase in network

intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane."[16]

86. In February 2014, Visa again warned Wendy's and other merchants of the increased risks posed by malware designed to target points-of-sale in an update to its August 2013 security alert. Specifically, the February 2014 alert stated:

> Visa is issuing this alert to make clients aware of new malware information and to remind Visa merchants to secure their payment processing (and non-payment) networks from unauthorized access. Visa highly recommends merchants implement these signatures on security solutions to detect a suspected breach. However, Visa recommends performing sufficient due diligence prior to implementing any block to avoid any inadvertent connectivity issues for legitimate access.[17]

87. In November 2015, Visa issued another security alert notifying Wendy's and other merchants of additional malware infections targeting and impacting merchants and restaurants. This alert specifically stated that a restaurant group had been targeted by this form of malware attack and that "infections started in August 2015 but appeared to increase dramatically in the middle of October 2015."[18] The security alert further stated that "Windows XP and Windows 7 (both 32 bit and 64 bit) are the primary operating systems infected." *Id.*

88. However, despite these numerous warnings and alerts, Wendy's failed to take reasonable steps to upgrade and protect Payment Card Data. Indeed, Wendy's has known for years

---

[16] Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware - *UPDATE* (August 2013), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf (last visited July 22, 2016).

[17] Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware - *UPDATE* (Feb. 2014), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf (last visited July 22, 2016).

[18] Security Alert, Visa, UPDATE - CYBER CRIMINALS TARGETING POINT OF SALE INTEGRATORS (Nov. 13, 2015), https://usa.visa.com/dam/VCOM/download/merchants/alert-pos-integrators.pdf (last visited July 22, 2016).

that a breach of its point-of-sale systems was possible and could cause serious disruption to its business and damage to payment card issuers. Specifically, Wendy's, in its Form 10-K filed with the SEC for the fiscal year ended December 28, 2014 ("2014 Form 10-K"), acknowledged that a data breach could adversely affect its business and operations:

> ***We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may result in adverse publicity and adversely affect the operation of our business and results of operations.***
>
> We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. A significant security breach of our computer systems or information technology could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, and incur penalties or other costs that could adversely affect the operation of our business and results of operations.[19]

[Emphasis in original].

89. Likewise, in its 2015 Form 10-K, Wendy's again listed as one of its potential risk factors, a data breach involving financial information from its point-of-sale systems:

> ***We are heavily dependent on computer systems and information technology and any material failure, interruption or security breach of our computer systems or technology could impair our ability to efficiently operate our business.***
>
> * * *
>
> Any security breach involving our or our franchisees' point-of-sale or other systems could result in a loss of consumer confidence and potential costs associated with fraud. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as

[19] The Wendy's Co., Annual Report (Form 10-K) (Feb. 26, 2015), https://www.sec.gov/Archives/edgar/data/30697/000003069715000003/twc10k2014.htm (last visited July 22, 2016).

> unauthorized access and computer viruses, may occur, resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. A security breach of our computer systems or information technology could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, and incur penalties or other costs that could adversely affect the operation of our business and results of operations.[20]

[Emphasis in original].

90. Despite acknowledging such risks, Wendy's disregarded the potential danger of a data breach by negligently failing to take adequate steps to prevent and stop hackers from gaining access to Wendy's computer systems. Wendy's also failed to prevent or mitigate damages by refusing to promptly disclose to financial institutions and the public the fact that a data breach had occurred.

2. Wendy's Ignored Warnings that Its Point-of-Sale System Was Vulnerable to a Data Breach

91. Prior to the data breach, Wendy's knew its data security systems were insufficient and that its point-of sale systems were vulnerable to a data breach. Accordingly, Wendy's had launched, but not completed, a mandatory upgrade to its point-of-sale systems in all restaurants to make it less susceptible to attack. However, due to Wendy's negligence, the upgrade was delayed, underfunded, and not completed in a timely fashion. Moreover, Wendy's should have begun the upgrade long before it actually did.

92. At the time of the data breach, the vast majority of Wendy's restaurants used the Aloha POS system, a third-party system developed by NCR Corp. ("NCR"), a global technology

[20] The Wendy's Co., Annual Report (Form 10-K) (Mar. 3, 2016), https://www.sec.gov/Archives/edgar/data/30697/000003069716000011/twc10k2015.htm (last visited July 22, 2016).

company. In 2009, Wendy's approved NCR as a supplier of point-of-sale technology for Wendy's restaurant system franchisees.[21]

93. According to the *DavCo* lawsuit between Wendy's and one of its major franchisees (discussed above), Wendy's announced plans in 2012 to implement the Aloha POS system as the required point-of-sale platform for all restaurants in the U.S. and Canada. Ex. 1, ¶¶16-18.

94. Unfortunately, the Aloha POS system was not much of an upgrade, as it was riddled with vulnerabilities – which Wendy's knew about before the data breach occurred.

95. For example, Wendy's franchisee, DavCo Restaurants LLC ("DavCo"), alleged in its counterclaim complaint ("DavCo Counterclaim") against Wendy's that the new Aloha POS system was fraught with serious technical and operational problems, which, according to DavCo, Wendy's acknowledged, but summarily dismissed as trivial. *See* DavCo Counterclaim, ¶9 (attached as Exhibit 2). DavCo alleged that the Aloha POS software was unstable and would repeatedly freeze and disconnect from the restaurant's network. *Id*., ¶¶25-30.

96. The shortcomings of the Aloha POS system were also publicly well-known by the time of the Wendy's data breach. A July 18, 2014 ComputerWorld article explained that "Matt Oh, a senior malware researcher with HP, recently bought a single Aloha point-of-sale terminal" and found:

> an eye-opening mix of default passwords, at least one security flaw and a leftover database containing the names, addresses, Social Security numbers and phone numbers of employees who had access to the system. His findings have received a fair amount of attention due to the role of such systems in high-profile data breaches at retailers including Target, Neiman Marcus and Michaels.[22]

---

[21] *NCR approved as POS vendor for Wendy's franchisees*, QSRWEB.COM (Dec. 8, 2009), http://www.qsrweb.com/news/ncr-approved-as-pos-vendor-for-wendys-franchisees/ (last visited July 22, 2016).

[22] Jeremy Kirk, *Aloha point-of-sale terminal, sold on eBay, yields security surprises*, COMPUTERWORLD (July 18, 2014, 6:15 AM (PST)), http://community.hpe.com/t5/Security-

97. According to the report, Oh "also found a memory-related problem known as a 'heap overflow' within a component called the Aloha Durable Messaging Service, which shuttles information between front-end and back-end systems. If exploited, the heap overflow 'could provide an attacker with full system level control of the target system[.]'" *Id.*

98. Moreover, in 2009, several restaurants in the U.S. that suffered data breaches sued the vendor and distributor of their Aloha POS systems. The lawsuit alleged that the Aloha POS system was non-compliant with industry standards (known as PCI DSS, discussed *infra*) and that hackers were able to install keyloggers and steal credit card numbers, resulting in hundreds of thousands of customers becoming victims of identity theft.[23] In fact, this lawsuit noted that, in 2007, Visa warned the vendor and distributor that the Aloha POS system unnecessarily stored sensitive cardholder data, making it non-compliant with PCI DSS and a vulnerable target for hackers. *Id.*

99. Similarly, in 2012, two Romanian hackers confessed that they had targeted over 150 Subway sandwich restaurants by breaking into Subway's Aloha POS system.[24]

3. Customization of the Aloha POS System Frequently Compromised Wendy's Point-of-Sale and Security Systems

100. Wendy's also knew that its point-of-sale systems were at risk for a potential data breach because customization of the Aloha POS system required Wendy's to either turn off or put

---

Research/Hacking-POS-Terminal-for-Fun-and-Non-profit/ba-p/6540620#.U8iJ1o2SzY8 (last visited July 22, 2016.

[23] Angela Moscaritolo, *Breached restaurateurs suing point-of-sale provider*, SC MAGAZINE (Dec. 2, 2009), http://www.scmagazine.com/breached-restaurateurs-suing-point-of-sale-provider/article/158892/ (last visited July 22, 2016).

[24] Adam Estes, *How Romanian Hackers Stole $10 Million From Subway Customers*, MOTHERBOARD.VICE.COM (Sept. 18, 2012, 12:30 PM) http://motherboard.vice.com/blog/how-two-guys-stole-10-million-from-subway-customers (last visited July 22, 2016).

in a less robust mode the point-of-sale security software that provided malware detection and other security services.

101. The Aloha POS system was designed for "table service" restaurants and required minimal customization to operate in that environment. Wendy's, however, had to significantly customize the Aloha POS system to operate in the "quick service," fast food environment. This customization was done piecemeal and on-the-fly, causing frequent system crashes that prevented essential point-of-sale and security systems from being fully operational for long stretches of time.

102. Tech Solutions Employee 1, who reported primarily to Wendy's Chief Information Officer, Don Zimmerman, said that the customization resulted in the Aloha POS system having recurring operational glitches, including system crashes. Tech Solutions Employee 1 explained that personnel involved in supporting the Aloha POS implementation process commonly complained about the unsystematic nature of the customizations, saying: "we're trying to build the ship as we're sailing it across the ocean."

103. Another former employee, who worked as a help desk specialist ("Help Desk Specialist"), agreed that the customization of the Aloha POS system was problematic because it hampered the system's overall functionality by creating conflicts between the Aloha POS system and Wendy's other IT systems.

104. According to the Help Desk Specialist, on a weekly or monthly basis, Wendy's internal point-of-sale development group would issue new software updates for the Aloha POS system. Typically, after these updates, the Help Desk Specialist said that calls to the help desk "would be exploding because [the update] broke something" and that this "happened all the time." The help desk staff often wondered what the point-of-sale development group was doing and would ask: "why do they keep breaking stuff?"

105. The Help Desk Specialist explained that Wendy's customization of the Aloha POS system frequently caused system crashes, as well as glitches, that prevented the Aloha POS system from properly authorizing and processing customer payment card transactions, due to loss of internet connectivity. When this occurred, restaurants were required to run point-of-sale transactions in "spool-down mode," which enabled transactions under $20 (in other words, the majority of Wendy's transactions) to be authorized until the restaurant in question could re-establish internet connectivity.

106. The Help Desk Specialist also noted that Solidcore, a software product that provided malware detection and other security functions for Wendy's Aloha POS system, used a significant amount of memory to properly operate. This severely impacted the performance and speed of other IT systems at Wendy's restaurants, including the Aloha POS system. In fact, the Aloha POS system frequently crashed due to this incompatibility.

107. Help Desk Specialist, as well as another former employee in the Technology Solutions group ("Tech Solutions Employee 2"), explained that, in order to troubleshoot problems with Solidcore, they would be required to either temporarily shut down Solidcore altogether or put Solidcore in a less robust, reduced-capacity mode. Help Desk Specialist was aware of several instances where Solidcore would remain offline for a significant amount of time because either the troubleshooting took a very long time to complete or the help desk specialist handling the assignment forgot to enable the system after troubleshooting was complete. With Solidcore offline, Payment Card Data was left entirely unprotected.

4. Wendy's Operated Its Point-of-Sale Registers on an Outdated, Unsupported Operating System that Was Susceptible to Data Breach

108. Wendy's further knew that its point-of-sale systems were at risk for a potential data breach because, as both Help Desk Specialist and Senior Engineer 2 confirmed, Wendy's point-of-sale registers were running on Windows XP, an outdated operating system.

109. In October 2013, an article titled "The End of Windows XP Could be the End for Your POS System" warned Aloha POS system users that "[i]f you're using a terminal that's a few years old, such as Micros or Aloha, it might be time to upgrade your POS system."[25] The article pointed out that point-of-sale systems, like Aloha POS, that utilized Windows XP were outdated and no longer supported by Microsoft.

110. In 2014, Microsoft, Windows XP's manufacturer, discontinued security updates and technical support for XP. Indeed, Microsoft published a specific warning to customers who continued to utilize Windows XP:

> After April 8, 2014, Microsoft will no longer provide security updates or technical support for Windows XP. Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. ***PCs running Windows XP after April 8, 2014, should not be considered to be protected***, and it is important that you migrate to a current supported operating system – such as Windows 10 – so you can receive regular security updates to protect their computer from malicious attacks.[26]

[Emphasis added].

111. Wendy's knew that XP-based point-of-sale registers were using outdated software and were beset with additional problems, yet failed to take necessary actions to upgrade their point-of-sale terminals.

---

[25] Adam Morgan, *The End of Windows XP Could be the End for Your POS System*, REVEL SYSTEMS (Oct. 1, 2013), http://revelsystems.com/blog/2013/10/01/end-windows-xp-end-pos-system/ (last visited July 22, 2016).

[26] *Support for Windows XP ended*, MICROSOFT (Apr. 8, 2014), https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support (last visited July 22, 2016).

5. Wendy's Lacked Adequate Firewall Protection and Appropriate Network Segmentation

112. Wendy's failed to maintain adequate firewall protection, which would have prevented its payment card systems from being breached by hackers. The System Admin, who was responsible for implementing network security upgrades at various corporate-owned and franchised restaurants, confirmed that that many of the restaurants he visited lacked any firewall whatsoever. The System Admin said other technicians likewise confirmed that certain Wendy's restaurants lacked any firewall.

113. Additionally, the System Admin identified problems associated with the Company's firewall configuration. For instance, when working on one upgrade project, the System Admin learned that the necessary routers had not been delivered to the restaurant sites. He advised his supervisor of the situation and his supervisor told him to go to Wal-Mart to buy "any router" he could find to use in the conversion. The System Admin cautioned his supervisor that any hacker could easily exploit this workaround and gain access to Payment Card Data. Ultimately, the System Admin refused to use routers purchased from Wal-Mart in the conversion. However, the System Admin remarked that some of his colleagues did, in fact, use these inappropriate routers. System Admin stated that using the Wal-Mart routers was "absolutely not" compliant with PCI DSS, which requires that parties install and maintain a firewall configuration to protect cardholder data, which the Wal-Mart routers would not do.

114. Indeed, Wendy's should have been aware of the PCI DSS requirements and the significant risks associated with a deficient or non-existent firewall and the risk that such deficiencies could lead to a data breach. Specifically, a Visa Data Security Alert, issued in February 2014, warned merchants, such as Wendy's, that they should be vigilant with respect to

their firewalls and firewall configuration. The February 2014 security alert informed merchants that they should:

> [r]eview your firewall configuration and ensure only allowed ports, services and IP (internet protocol) addresses are communicating with your network. This is especially critical on outbound (e.g., egress) firewall rules, where compromised entities allow ports to communicate to any IP on the Internet. Hackers will leverage this misconfiguration to exfiltrate data to their IP address.[27]

Despite this, Wendy's failed to take necessary measures to maintain an adequate firewall that was properly configured to prevent hackers from penetrating its computer network.

115. Wendy's also lacked proper network segmentation to prevent a user, with access to one area of the network, from accessing areas of the network where Payment Card Data would be transmitted or stored. The System Admin explained that Wendy's maintained two (or dual) networks and that both were connected to the Aloha POS system. The System Admin further stated that dual networks lacked proper network segmentation, which would allow a hacker, who could gain access to one area of the network, to access other areas of the network to steal Payment Card Data. The System Admin was certain that Wendy's dual network configuration was not compliant with PCI DSS because Payment Card Data was not adequately separated from Wendy's public wireless internet network.

116. The System Admin further stated that he was performing a network security upgrade in 2015 to render Wendy's IT environment less penetrable, specifically by improving the firewall protection and separating Payment Card Data from Wendy's public wireless internet network. At the time of his departure from Wendy's, in February 2016, the System Admin stated there remained hundreds of Wendy's establishments that needed to perform the network security

---

[27] Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware - *UPDATE* (Feb. 2014), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf (last visited July 22, 2016).

upgrade, which included proper network segmentation. Thus, hundreds of restaurants had inadequate security at the time of the data breach because Wendy's failed to timely implement the necessary changes and upgrades.

117. Another former Wendy's employee, who worked as a Senior Engineer in Restaurant Infrastructure ("Senior Engineer 1"), also identified that there were network segmentation issues with respect to the setup of the servers at Wendy's restaurants. He explained that all devices with electronic connectivity, including point-of-sale terminals and electronic menu board displays, resided on the same network. Therefore, anyone who could gain access to the network would be able to also have access to Payment Card Data. Senior Engineer 1 believed that Wendy's violated PCI DSS because Payment Card Data was not properly segmented from other, non-sensitive information.

118. Senior Engineer 1 stated that every Wendy's restaurant that was using the Aloha POS system, regardless of whether it was a franchise or company-owned store, was connected to the Aloha Command Center. This allowed Wendy's corporate headquarters to have access to each restaurant running the Aloha POS system. The Aloha Command Center also allowed the Company to monitor the status of each server and point-of-sale terminal and provide access to render technical or other support to Aloha POS system users. Senior Engineer 1 further stated that the corporate data center, which was housed on a server at the Company's headquarters, included the Aloha Command Center software that ran on all stores utilizing the Aloha POS system. This configuration demonstrates that, without proper network segmentation, there was full electronic connectivity between corporate and its franchisees. As a result of this connectivity, and the lack of adequate firewall protection and appropriate network segmentation, a hacker not only could

enter Wendy's computer network, but also would be able to jump unhindered between various network platforms and ultimately access Wendy's customers' Payment Card Data.

6. Wendy's Failed to Implement Protocols that Would Have Protected Payment Card Data

119. Wendy's failed to implement certain protocols, such as software image hardening, password protecting programs that captured Payment Card Data, and encrypting Payment Card Data at the point of sale. These protocols would have detected and prevented unauthorized programs from being installed on Wendy's point-of-sale systems and otherwise would have protected Payment Card Data in the event of a data breach.

120. For instance, software hardening requires a company to remove unnecessary applications and processes from software, which enables the company to control what applications can run on the point-of-sale system to prevent unauthorized access and attack. Senior Engineer 1 was responsible for making sure that images of the software that were released and deployed to all restaurants using the Aloha POS system met PCI DSS standards (as described below). Senior Engineer 1 was responsible for analyzing images from all of the devices in use in the restaurants, including point-of-sale terminals, kitchen devices, and back office servers – all of which were running Aloha POS software and were connected to Payment Card Data. Senior Engineer 1 stated that, if images of the software were not hardened, it could allow Payment Card Data to be "exfiltrated," or stolen, from the system. Senior Engineer 1 was aware that Wendy's had not hardened the system images successfully and believed this made Wendy's vulnerable to a data breach.

121. After Senior Engineer 1 left Wendy's, and immediately before the data breach, he said the person who took over primary responsibility for ensuring that images were both hardened and released was not qualified for the job. Senior Engineer 1 said that his replacement would call

him nearly every day for help with the imaging process. From these discussions, Senior Engineer 1 knew that the images of the software were not properly hardened and contained many mistakes, rendering the Aloha POS systems susceptible to a potential data breach.

122. Senior Engineer 2 confirmed that, prior to the data breach, none of the versions of the Aloha POS software Wendy's was deploying were hardened. Senior Engineer 2, like Senior Engineer 1, believed that because the Aloha POS software was not hardened, the IT systems at Wendy's restaurants were not secure and were not PCI DSS compliant.

123. The lack of image hardening was further buttressed by the fact that the Payment Card Data was unencrypted at the point-of-sale terminal, which would have prevented exfiltrated Payment Card Data from being publicly exposed.[28] Senior Engineer 1 explained that, although the electronic data capture ("EDC") file containing Payment Card Data would be encrypted during its transfer between an Aloha POS terminal and the bank authorizing the transaction, Payment Card Data existed in an unencrypted format on the Aloha POS terminals.

124. Senior Engineer 1 said that the EDC file containing Payment Card Data would be accessible remotely by anyone using the Aloha Command Center software. Importantly, Senior Engineer 1 further stated that the user identification and passwords associated with these EDC files were not encrypted and thus, could be stolen by hackers to unencrypt any later-encrypted Payment Card Data.

125. Senior Engineer 2 identified Wendy's password management as another potential weakness in Wendy's computer system. He explained that the same passwords were used across

[28] Chloe Green, *Point of Sale malware takes a bite out of Wendy's fast food chain*, INFORMATIONAGE (June 10, 2016), http://www.information-age.com/technology/security/123461588/point-sale-malware-takes-bite-out-wendys-fast-food-chain (last visited July 22, 2016).

certain devices and that "any former employee with an axe to grind" could cause significant damage to Wendy's, since Wendy's did not regularly, if ever, change these generic passwords.

7. Wendy's Failed to Install Software to Adequately Track and Monitor Its Network

126. Wendy's failed to adequately track access to its network and to monitor the network for unusual activity, particularly with respect to its point-of-sale terminals, which would have allowed Wendy's to detect and potentially prevent hackers from stealing Payment Card Data. One software vendor, Symantec, provides the following explanation regarding its endpoint protection software: "Symantec's network threat protection technology analyzes incoming data and blocks threats while they travel through the network before hitting endpoints. Rules-based firewall and browser protection are also included to protect against web-based attacks."[29]

127. Specifically, had Wendy's implemented proper endpoint detection and prevention systems, it would have been able to identify suspicious activity occurring within Wendy's network. Additionally, proper endpoint detection would have triggered warnings and alerted Wendy's to the transmission of Payment Card Data within its systems and should have alerted Wendy's to large volumes of data being removed, or exfiltrated, from its network.

8. Wendy's Failed to Upgrade Its Payment Systems to Utilize EMV Technology

128. The payment card industry also set rules requiring all businesses to upgrade to new card readers that accept EMV chips. EMV chip technology uses imbedded computer chips instead of magnetic strips, to store Payment Card Data. Unlike magnetic-strip cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is

[29] Data Sheet, Symantec Corporation, Symantec™ Endpoint Protection 12.1.6 (2015), https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-en.pdf (last visited July 22, 2016).

used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the thieves, making it much more difficult for criminals to profit from what is stolen.

129. The payment card industry (MasterCard, Visa, Discover, and American Express) set a deadline of October 1, 2015 for businesses to transition their systems from magnetic-strip to EMV technology. Wendy's did not meet that deadline.

130. Under Card Operating Regulations, businesses accepting payment cards, but not meeting the October 1, 2015 deadline, agree to be liable for damages resulting from any data breaches.

D. Wendy's Failed to Comply with Its Duties

1. Wendy's Failed to Comply with Industry Standards for Data Security

131. As the foregoing demonstrates, Wendy's failed to comply with industry standards for data security.

132. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit Payment Card Data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of Payment Card Data, although it sets the minimum level of what must be done, not the maximum.

133. PCI DSS 3.1, the version of the standards in effect at the time of the data breach, imposed the following 12 "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Furthermore, PCI DSS 3.1 set forth detailed and comprehensive requirements that had to be followed to meet each of the 12 mandates.

134. Among other things, PCI DSS required Wendy's to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; to timely upgrade its point-of-sale software; implement proper network segmentation; encrypt Payment Card Data at the point-of-sale; restrict access to Payment Card Data to those with a need to know; and establish a process to identify; and timely fix security vulnerabilities. As discussed above, Wendy's failed to comply with each of these requirements.

2. Wendy's Failed to Comply with Federal Trade Commission Requirements

135. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by §5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. §45.

136. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

137. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

138. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

139. In the years leading up to the Wendy's data breach, and during the course of the breach itself, Wendy's failed to follow the guidelines set forth by the FTC. Furthermore, by failing to have reasonable data security measures in place, Wendy's engaged in an unfair act or practice within the meaning of §5 of the FTC Act.

3. Wendy's Failed to Follow Its Own Policies and Procedures

140. At the time of the breach, Wendy's internal policies and procedures required that customer information be kept confidential, system vulnerabilities be mitigated in a timely manner, necessary software upgrades be implemented, and data be encrypted.

141. Wendy's violated these policies and procedures in the time leading up to the Wendy's data breach, and during the commission of the breach itself, by failing to maintain the confidentiality of its customer information, mitigate system vulnerabilities in a timely manner, upgrade software security, and encrypt Payment Card Data at the point-of-sale.

142. Wendy's maintains a Code of Business Conduct and Ethics ("Code"), which was last updated and approved by the Wendy's Board of Directors on December 13, 2011. This Code provides, in relevant part, that:

> Information about a franchisee's or supplier's business is confidential as is personal information about customers. Disclosure within the Company should only be on a business 'need to know' basis. Disclosure to outsiders, except to comply with legal requirements, is not only inconsistent with this Code but in some cases may be illegal.[30]

143. Wendy's plainly failed to fulfill its own internal information security policy.

E. The Data Breach Damaged Financial Institutions

144. Wendy's failed to protect its customers' Payment Card Data and as a result, the FI Plaintiffs and Class members have suffered millions of dollars in damages

145. Wendy's failed to follow industry standards and failed to effectively monitor its point-of-sale and security systems to ensure the safety of customer information. Wendy's substandard security protocols, improper retention of cardholder data, and failure to regularly monitor for unauthorized access caused customers' Payment Card Data to be compromised for months without detection by Wendy's.

146. The data breach caused substantial damage to the FI Plaintiffs and Class members, who had to act immediately to mitigate the massive number of fraudulent transactions being made

[30] The Wendy's Company, *Code of Conduct* (Dec. 13, 2011), http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-govconduct (last visited July 22, 2016).

on payment cards that they had issued while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but the FI Plaintiffs and Class members are not. Financial institutions, like the FI Plaintiffs and other Class members, bear primary responsibility for reimbursing customers for fraudulent charges and covering the cost of issuing new cards for customers to use.

147. As a result of the Wendy's data breach, the FI Plaintiffs and Class members were required, and will continue to be required, to cancel and reissue payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their customers. Plaintiffs and members of the Class also lost interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to the FI Plaintiffs and Class members – as well as the account numbers on the face of the cards – were devalued.

148. The financial damages suffered by the FI Plaintiffs and members of the Class are significant and ongoing. Industry sources estimate that millions of accounts could be affected by the data breach.

V. CLASS ACTION ALLEGATIONS

149. The FI Plaintiffs bring this action on behalf of themselves and as a class action, pursuant to the provisions of Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, on behalf of the following class (the "Class"):

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from Wendy's from October 1, 2015 to the present.

150. Excluded from the Class are Defendants and their subsidiaries and affiliates; all employees of Defendants; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

151. Certification of the FI Plaintiffs' claims for Class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a), (b)(2)-(3) are satisfied. The FI Plaintiffs can prove the elements of their claims on a Class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

152. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While the FI Plaintiffs are informed and believe that there are thousands of members of the Class, the precise number of Class members is unknown to the FI Plaintiffs. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

153. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. whether Defendants engaged in the misconduct alleged herein;

b. whether Wendy's owed a duty to the FI Plaintiffs and members of the Class to protect Payment Card Data;

c. whether Wendy's failed to provide adequate security to protect Payment Card Data;

d. whether Wendy's negligently, or otherwise improperly, allowed third parties to access Payment Card Data;

e. whether Wendy's failed to adequately notify the FI Plaintiffs and members of the Class that its computer systems were breached;

f. whether the FI Plaintiffs and members of the Class were injured and suffered damages and ascertainable losses;

g. whether Wendy's failure to provide adequate security proximately caused the FI Plaintiffs' and Class members' injuries;

h. whether the FI Plaintiffs and members of the Class are entitled to damages and, if so, the measure of such damages; and

i. whether the FI Plaintiffs and members of the Class are entitled to declaratory and injunctive relief.

154. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. The FI Plaintiffs are members of the Class, having issued payment cards that were compromised in the Wendy's data breach. The FI Plaintiffs' claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' conduct.

155. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. The FI Plaintiffs are adequate Class representatives because they are members of the Class and their interests do not conflict with the interests of the other members of the Class that they seek to represent. The FI Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interests in mind. The FI Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and the FI Plaintiffs intend to

prosecute this action vigorously. The FI Plaintiffs, and their counsel, will fairly and adequately protect the Class's interests.

156. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in each FI Plaintiff's individual case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by the FI Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

157. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendants have acted, or refused to act, on grounds generally applicable to the Class making final declaratory or injunctive relief appropriate.

VI. CHOICE OF LAW

158. Wendy's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Ohio and the tortious and deceptive acts complained of occurred in, and radiated from, Ohio.

159. The key wrongdoing at issue in this litigation (Wendy's failure to employ adequate data security measures) emanated from Wendy's headquarters in Ohio. Indeed, Wendy's admits in the *DavCo* lawsuit that one of the initiatives at issue in this case – the implementation of a common point of sale platform – was "conceived and developed and are being administered by Wendy's primarily in Ohio." Ex. 1, ¶6.

160. Wendy's point-of-sale system and IT personnel operate out of and are located at Wendy's headquarters in Ohio. For example, Wendy's currently is hiring for a number of positions within the IT Security department based in Dublin, Ohio, including, *inter alia*, a POS Solutions Manager to investigate reported issues with the Aloha POS system;[31] an Endpoint Security Sr. Engineer to handle administration, maintenance, and support of endpoint security tools and to ensure PCI compliance by recommending and implementing adjustments to the security of endpoints based on the current PCI requirements;[32] and an ETL Sr. Developer to modify and create components for the Enterprise Data Warehouse, including design and documentation of system standards.[33]

161. Ohio, which seeks to protect the rights and interests of Ohio and other U.S. businesses against a company doing business in Ohio, has a greater interest in the claims of

---

[31] Job Posting, The Wendy's Company, Analyst - POS Solutions * The Wendy's Company, Dublin, OH, https://wendys.taleo.net/careersection/ro/jobdetail.ftl?job=127580&src=JB%AD110401/2 (last visited July 22, 2016).

[32] Job Posting, The Wendy's Company, Sr. Engineer - Endpoint Security * The Wendy's Company, Dublin, OH, https://wendys.taleo.net/careersection/ro/jobdetail.ftl?job=122760&src=JB%AD110401/2 (last visited July 22, 2016).

[33] Job Posting, The Wendy's Company, Sr Developer - Analytics * The Wendy's Company, Dublin, OH, https://wendys.taleo.net/careersection/ro/jobdetail.ftl?job=127621&src=JB%AD110401/3 (last visited July 22, 2016).

Plaintiffs and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

162. Application of Ohio law to a nationwide Class with respect to Plaintiffs' and the Class members' claims is neither arbitrary nor fundamentally unfair because Ohio has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs and the nationwide Class.

163. The location where Plaintiffs were injured was fortuitous and Wendy's could not have foreseen where the injury would take place, as Wendy's didn't know which banks Wendy's customers used and the location of these banks' headquarters, or principal places of business, at the time of the breach.

VII. CAUSES OF ACTION

COUNT I
Negligence
On behalf of the FI Plaintiffs and the Class

164. The FI Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

165. Wendy's owed – and continues to owe – a duty to the FI Plaintiffs and the Class to use reasonable care in safeguarding Payment Card Data and to notify them of any breach in a timely manner, so that compromised financial accounts and credit cards can be closed quickly in order to avoid fraudulent transactions. This duty arises from several sources, including, but not limited to, the sources described below, and is independent of any duty Wendy's owed as a result of its contractual obligations.

166. Wendy's has a common law duty to prevent the foreseeable risk of harm to others, including the FI Plaintiffs and the Class. It was certainly foreseeable to Wendy's that injury would

result from a failure to use reasonable measures to protect Payment Card Data and to provide timely notice that a breach was detected. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of Wendy's customers; thieves would use Payment Card Data to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud by cancelling and reissuing the compromised cards and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

167. Wendy's assumed the duty to use reasonable security measures as a result of its conduct.

168. In addition to its general duty to exercise reasonable care, Wendy's also had a duty of care as a result of the special relationship that existed between Wendy's and the FI Plaintiffs and members of the Class. The special relationship arose because financial institutions entrusted Wendy's with Payment Card Data. Only Wendy's was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

169. Wendy's duty to use reasonable data security measures also arose under §5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as Wendy's. The FTC publications and data security breach orders described above further form the basis of Wendy's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of Wendy's.

170. Wendy's duty to use reasonable care in protecting Payment Card Data arose not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

171. Wendy's breached its common law, statutory, and other duties and thus, was negligent by failing to use reasonable measures to protect the FI Plaintiffs' Payment Card Data from the hackers who perpetrated the data breach and by failing to provide timely notice of the breach. Upon information and belief, the specific negligent acts and omissions committed by Wendy's include, but are not limited to, some, or all, of the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems to protect against malware;

c. failure to comply with industry standards for software and point-of-sale security;

d. failure to regularly update its antivirus software;

e. failure to maintain an adequate firewall;

f. failure to track and monitor access to its network and cardholder data;

g. failure to limit access to those with a valid purpose;

h. failure to encrypt Payment Card Data at the point-of-sale;

i. failure to transition to the use of EMV technology;

j. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

k. failure to assign a unique ID to each individual with access to its systems;

l. failure to automate the assessment of technical controls and security configuration standards;

m. failure to adequately staff and fund its data security operation;

n. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

o. failure to recognize red flags signaling that Wendy's systems were inadequate and that, as a result, the potential for a massive data breach was increasingly likely;

p. failure to recognize that hackers were stealing Payment Card Data from its network while the data breach was taking place; and

q. failure to disclose the data breach in a timely manner.

172. In connection with the conduct described above, Wendy's acted wantonly, recklessly, and with complete disregard for the consequences.

173. As a direct and proximate result of Wendy's negligence, the FI Plaintiffs and members of the Class have suffered, and continue to suffer, injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. The FI Plaintiffs and the Class also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT II
Negligence *Per Se*
On behalf the FI Plaintiffs and the Class

174. The FI Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

175. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wendy's, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Wendy's duty.

176. Wendy's violated §5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Card Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Wendy's conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at an international restaurant, including, specifically, the immense damages that would result to consumers and financial institutions.

177. Wendy's violation of §5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

178. The FI Plaintiffs and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses. Moreover, many of the Class members are credit unions, which are organized as cooperatives whose members are consumers.

179. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by the FI Plaintiffs and the Class.

180. As a direct and proximate result of Wendy's negligence *per se*, the FI Plaintiffs and the Class have suffered, and continue to suffer, injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT III
Violation of the Ohio Deceptive Trade Practices Act ("Ohio DTPA")
Ohio Rev. Code §§ 4165.01, *et seq.*
On behalf the FI Plaintiffs and the Class

181. The FI Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

182. The FI Plaintiffs and Wendy's are "persons" within the meaning of Ohio Rev. Code § 4165.01(D).

183. Wendy's engaged in "the course of [its] business" within the meaning of Ohio Rev. Code § 4165.02(A) with respect to the acts alleged herein.

184. The Ohio DTPA, Ohio Rev. Code § 4165.02(A), provides that a "person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation," the person does any of the following: "(7) Represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have . . . [Or]; (9) Represents that goods or services are of a particular standard, quality, or grade . . . , if they are of another."

185. In the course of Wendy's business, Wendy's misrepresented the security of its point of sale payment systems and engaged in deceptive trade practices. The FI Plaintiffs and members of the Class had no way of discerning that Wendy's representations were false and deceptive because Wendy's controlled information regarding its security practices and procedures and the safety of its POS systems and cardholder data environment ("CDE.").

186. Compliance with PCI DSS is required for all businesses that handle credit or debit card payments. Simply by being an active participant in the payment card networks, Wendy's represented that it is PCI compliant, and never disclosed that it was not PCI compliant. The FI Plaintiffs and Class members, as issuers of payment cards, know that PCI compliance is the industry standard and expect and rely on all merchants, including Wendy's, to be PCI compliant in order to ensure the security of their payment cards used at the merchants' establishments.

187. The foregoing allegations and witness statements evidence that Wendy's was in fact not PCI compliant at the time of the breach.

188. In addition, Wendy's made specific false and misleading representations regarding the security of its payment card systems. For example, in 2014, Wendy's, by and through its franchisees (including, but not limited to, DavCo and WendCentral Corp.), authorized disclosure of public statements, which represented that Wendy's restaurants were PCI DSS compliant and that payment card systems would be secure. This was false, as detailed in the foregoing allegations.

189. Furthermore, on May 11, 2016, Wendy's made a disclosure to the SEC that contained the following statements:

> Based on the preliminary findings of the investigation and other information, the Company believes that malware, installed through the use of compromised third-party vendor credentials, ***affected one particular point of sale system at fewer than 300 of approximately***

> ***5,500 franchised North America Wendy's restaurants***, starting in the fall of 2015. ***These findings also indicate that the Aloha point of sale system has not been impacted by this activity***. The Aloha system is already installed at all Company-operated restaurants and in a majority of franchise-operated restaurants, with implementation throughout the North America system targeted by year-end 2016. The Company expects that it will receive a final report from its investigator in the near future.
>
> The Company has worked aggressively with its investigator to identify the source of the malware and quantify the extent of the malicious cyber-attacks, and ***has disabled and eradicated the malware in affected restaurants***.[34]

[Emphasis added.]

190. In the foregoing statement, Wendy's represented that at least 5,200 of its restaurants were not affected by the data compromise, which was not true.

191. In the foregoing statement, Wendy's represented that the Aloha point of sale system was not impacted by the data compromise, which was not true.

192. In the foregoing statement, Wendy's represented that the malware on the point of sale systems at its restaurants had been disabled and eradicated by May 11, 2016, which was not true.

193. Wendy's thus violated the provisions of the Ohio DTPA, at a minimum by: (1) representing that its POS systems and CDE had characteristics, uses, benefits, and qualities which they did not have; and/or (2) representing that its POS systems and CDE were of a particular standard, quality, and grade, adequate to protect Payment Card Data, when they were not.

---

[34] The Wendy's Co., Current Report (EX-99.1 to Form 8-K) (May 11, 2016), https://www.sec.gov/Archives/edgar/data/30697/000119312516586362/d158377dex991.htm (last visited July 22, 2016).

194. Wendy's unfair or deceptive acts or practices were likely to and did in fact deceive FI Plaintiffs, members of the Class, and the public about the likelihood that Payment Card Data would be compromised due to Wendy's inadequate security measures.

195. Due to the significant control over franchisees exercised by Wendy's, particularly with respect to its point of sale payment systems, Wendy's franchisees acted as Wendy's agents when making statements regarding the security and compliance status of the payment of sale systems at the respective franchised Wendy's locations.

196. The FI Plaintiffs and members of the Class suffered ascertainable loss and actual damages as a direct and proximate result of Wendy's false, deceptive, and misleading statements, including costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

197. Wendy's had an ongoing duty to all financial institutions, including the FI Plaintiffs and members of the Class, to refrain from unfair and deceptive practices under the Ohio DTPA in the course of its business.

198. Wendy's violations present a continuing risk to the FI Plaintiffs as well as to the general public.

199. Wendy's unlawful acts and practices complained of herein affect the public interest.

200. Pursuant to Ohio Rev. Code § 4165.03, Plaintiffs seek an order enjoining Wendy's unfair or deceptive acts or practices, damages, punitive damages, and attorneys' fees, costs, and any other just and proper relief available under the Ohio DTPA.

COUNT IV
Declaratory and Injunctive Relief
On behalf of Plaintiffs and the Class

200. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

201. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

202. An actual controversy has arisen in the wake of Wendy's data breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiffs allege that Wendy's data security measures were inadequate and remain inadequate. Wendy's denies these allegations. Furthermore, Plaintiffs continue to suffer injury as additional fraudulent charges are being made on payment cards they issued to Wendy's customers.

203. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Wendy's continues to owe a legal duty to secure its customers' personal and financial information – specifically including information pertaining to credit and debit cards used by Wendy's customers – and to notify financial institutions of a data breach under the common law, §5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;

b. Wendy's continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Wendy's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

204. The Court also should issue corresponding injunctive relief requiring Wendy's to employ adequate security protocols, consistent with industry standards, to protect its Payment Card Data. Specifically, this injunction should, among other things, direct Wendy's to:

a. utilize industry standard encryption to encrypt the transmission of cardholder data at the point-of-sale and at all other times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

h. install all upgrades recommended by manufacturers of security software and firewalls used by Wendy's.

205. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Wendy's. The risk of another such breach is real, immediate, and substantial. If another breach at Wendy's occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for out of pocket

damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

206. The hardship to Plaintiffs and the Class, if an injunction is not issued, exceeds the hardship to Wendy's, if an injunction is issued. Among other things, if another massive data breach occurs at Wendy's, Plaintiffs and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Wendy's of complying with an injunction by employing reasonable data security measures is relatively minimal and Wendy's has a pre-existing legal obligation to employ such measures.

207. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Wendy's, thus eliminating the injuries that would result to Plaintiffs, the Class, and the millions of consumers whose confidential information would be compromised.

208. Each Association Plaintiff participates in this lawsuit on behalf of its members. Each Association Plaintiff seeks, where its members are entitled to do so and the claims for relief otherwise permit, the declaratory and injunctive relief requested above on behalf of each Association Plaintiff's members who will continue to suffer as a result of Wendy's conduct unless it is stopped.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court:

A. Certify the Class and appoint the FI Plaintiffs and Plaintiffs' counsel to represent the Class;

B. Enter a monetary judgment in favor of the FI Plaintiffs and members of the Class to compensate them for the injuries suffered, together with pre-judgment and post-judgment interest, treble damages, and penalties where appropriate;

C. Enter a declaratory judgment in favor of Plaintiffs and the Class, as described above;

D. Grant Plaintiffs the injunctive relief requested;

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable.

Dated: July 22, 2016

s/ Gary F. Lynch
Gary F. Lynch
Jamisen A. Etzel
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburg, PA 15222
Telephone: (412) 253-6307
Facsimile: (412) 322-9243
glynch@carlsonlynch.com
jetzel@carlsonlynch.com

Erin Green Comite
Joseph P. Guglielmo
Stephen J. Teti
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
The Chrysler Building
405 Lexington Avenue, 40th Floor
New York, NY 10174
Telephone: (212) 223-6444

Facsimile: (212) 223-6334
ecomite@scott-scott.com
jguglielmo@scott-scott.com
steti@scott-scott.com

Co-Lead Counsel for Plaintiffs

Karen Hanson Riebel
Kate Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 596-4097
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

James J. Pizzirusso
Swathi Bojedla
HAUSFELD, LLP
1700 K. Street, NW, Suite 650
Washington, DC 20006
Telephone: (202) 540-7200
Facsimile: (202) 540-7201
jpizzirusso@hausfeldllp.com
sbojedla@hausfeldllp.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2921
bbleichner@chestnutcambronne.com

Arthur M. Murray
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Telephone: (504) 525-8100
Facsimile: (504) 584-5249
amurray@murray-lawfirm.com

Brian C. Gudmundson
ZIMMERMAN REED, LLP
1100 IDS Center

80 South 8th Street
Minneapolis, MN 55042
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com

Plaintiffs' Executive Committee